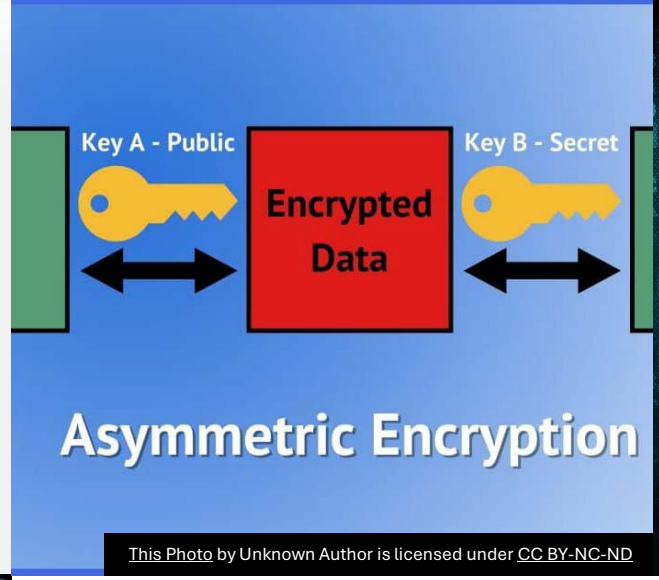
Zaštita podataka u e-poslovanju

Elektronsko poslovanje

UVOD



E-poslovanje podrazumeva elektronsku razmenu informacija i transakcija preko interneta. Bezbednost podataka u ovom kontekstu je od suštinskog značaja, jer uključuje osetljive informacije kao što su:

- lični podaci korisnika,
- informacije o platnim karticama,
- poslovne i trgovinske tajne.

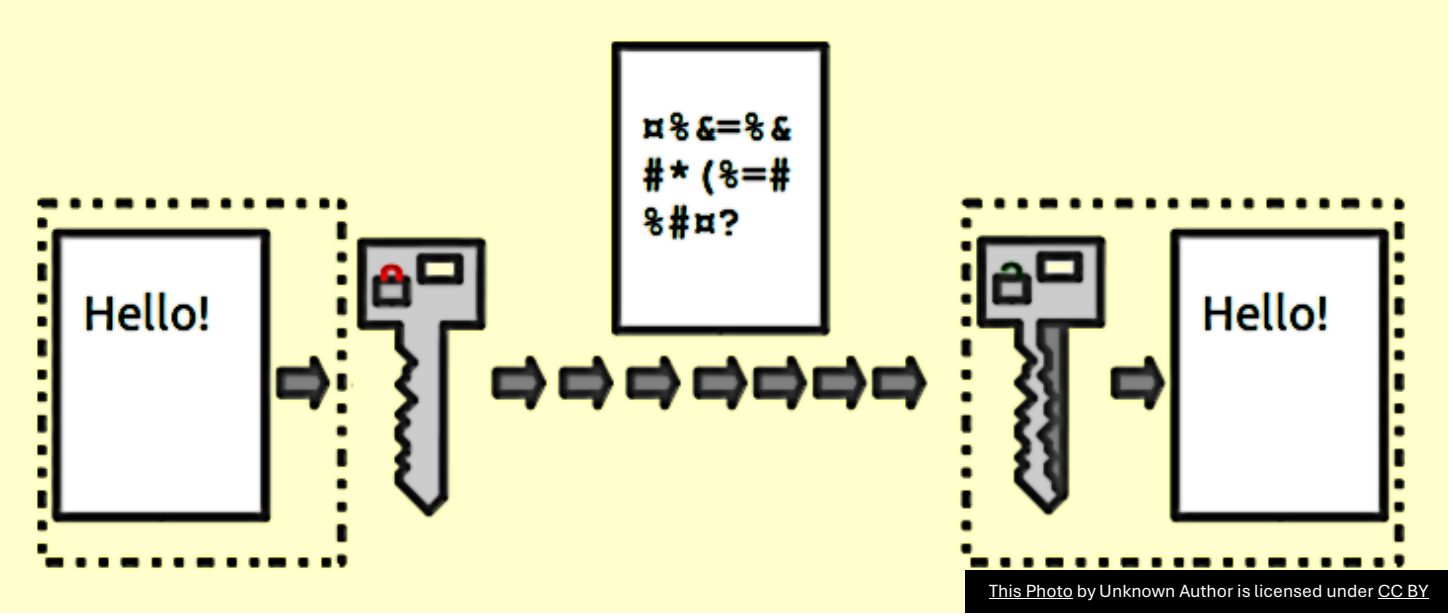
Osnovni principi zaštite podataka

1. **Poverljivost (Confidentiality)-** sprečavanje neovlašćenog pristupa podacima.
2. **Integritet (Integrity)n-** osiguranje da podaci nisu izmenjeni ili kompromitovani.
3. **Dostupnost (Availability)-** omogućavanje da podaci budu dostupni ovlašćenim korisnicima kad god su potrebni.
4. **Autentičnost (Authenticity)-** potvrda identiteta učesnika u komunikaciji.
5. **Neosporivost (Non-repudiation)-** sprečavanje poricanja poslatih ili primljenih poruka.

Mehanizmi zaštite

- Enkripcija podataka (simetrična i asimetrična),
- Sertifikati i digitalni potpisi,
- Protokoli kao što su HTTPS, SSL/TLS,
- Sistemi za kontrolu pristupa i autentifikaciju (npr. dvofaktorska autentifikacija),
- Zaštita od napada (npr. DoS, phishing, man-in-the-middle).

Enkripcija podataka



- **Enkripcija** (šifrovanje) je proces pretvaranja čitljivih podataka (plaintext) u nečitljiv oblik (ciphertext) kako bi se zaštitili od neovlašćenog pristupa.

Simetrična enkripcija

Isti ključ se koristi za **šifrovanje i dešifrovanje** podataka.

Primer algoritama:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- RC4, Blowfish

Kako funkcioniše AES?

- AES radi sa **fiksnim blokovima podataka od 128 bita** i koristi **ključeve dužine 128, 192 ili 256 bita**. Proces se sastoji od više rundi (10, 12 ili 14 – u zavisnosti od dužine ključa).

Faze AES enkripcije

1. **Dodavanje početnog ključa (AddRoundKey):**

   Ulazni blok (plaintext) se kombinuje sa početnim ključem pomoću XOR operacije.

2. **Glavne runde (ponavlja se više puta):**

   SubBytes - Zamena bajtova preko S-box funkcije.

   ShiftRows - Rotacija redova matrice bajtova.

   MixColumns - Kombinovanje kolona radi difuzije podataka.

   AddRoundKey - Ponovna XOR operacija sa rundnim ključem.

3. **Završna runda:**

   Kao glavna runda, ali **bez MixColumns**.

Zašto je AES bezbedan?

S-box funkcija štiti od linearne i diferencijalne kriptanalize.

Višerundna struktura otežava pokušaje razbijanja šifre.

Efikasan i brz algoritam – široko korišćen u VPN-ovima, HTTPS protokolu, bežičnim mrežama (npr. WPA2), i fajl enkripciji.

Šta je DES?

- DES (Data Encryption Standard) je prvi standardizovani algoritam simetrične enkripcije.
- Koristi 64-bitne blokove i 56-bitni ključ.
- Razvijen 1970-ih i korišćen decenijama u vladinim i industrijskim sistemima.
- Danas se smatra nesigurnim zbog kratkog ključa i naprednih napada.

Faze DES algoritma

1. Početna permutacija (IP)
2. 16 rundi enkripcije koristeći Feistel strukturu:
- Ekspanzija, XOR sa rundnim ključem, S-box zamena i permutacija
3. Završna permutacija (IP-1)

Kombinuje deljenje bloka na leve i desne polovine tokom procesa.

Upotreba i sigurnost DES-a

- DES je bio široko korišćen u bankarstvu i bezbednosnim sistemima.
- Danas je zastareo – podložan brute-force napadima.
- Zamenjen AES-om i Triple DES (3DES).
- 3DES koristi DES algoritam tri puta radi povećanja sigurnosti.

RC4 (Rivest Cipher 4)

- Stream cipher algoritam razvijen od strane Rona Rivesta 1987. godine.
- Koristi varijabilnu dužinu ključa (od 40 do 2048 bita).
- Brz i jednostavan za implementaciju – korišćen u WEP, SSL/TLS protokolima.
- Sigurnost kompromitovana – poznati napadi na slabosti algoritma.

Blowfish

- Simetrični blokovski algoritam razvijen od Bruce Schneier-a 1993. godine.
- Koristi 64-bitne blokove i ključeve dužine do 448 bita.
- Dizajniran kao brza i sigurna alternativa DES-u.
- Pogodan za aplikacije koje ne zahtevaju česte promene ključa.
- Zamena: Twofish (moderniji naslednik Blowfish algoritma).

Infrastruktura javnog ključa (PKI – Public Key Infrastructure)

- PKI je sistem koji omogućava bezbednu elektronsku komunikaciju kroz upotrebu kriptografije sa javnim ključem.

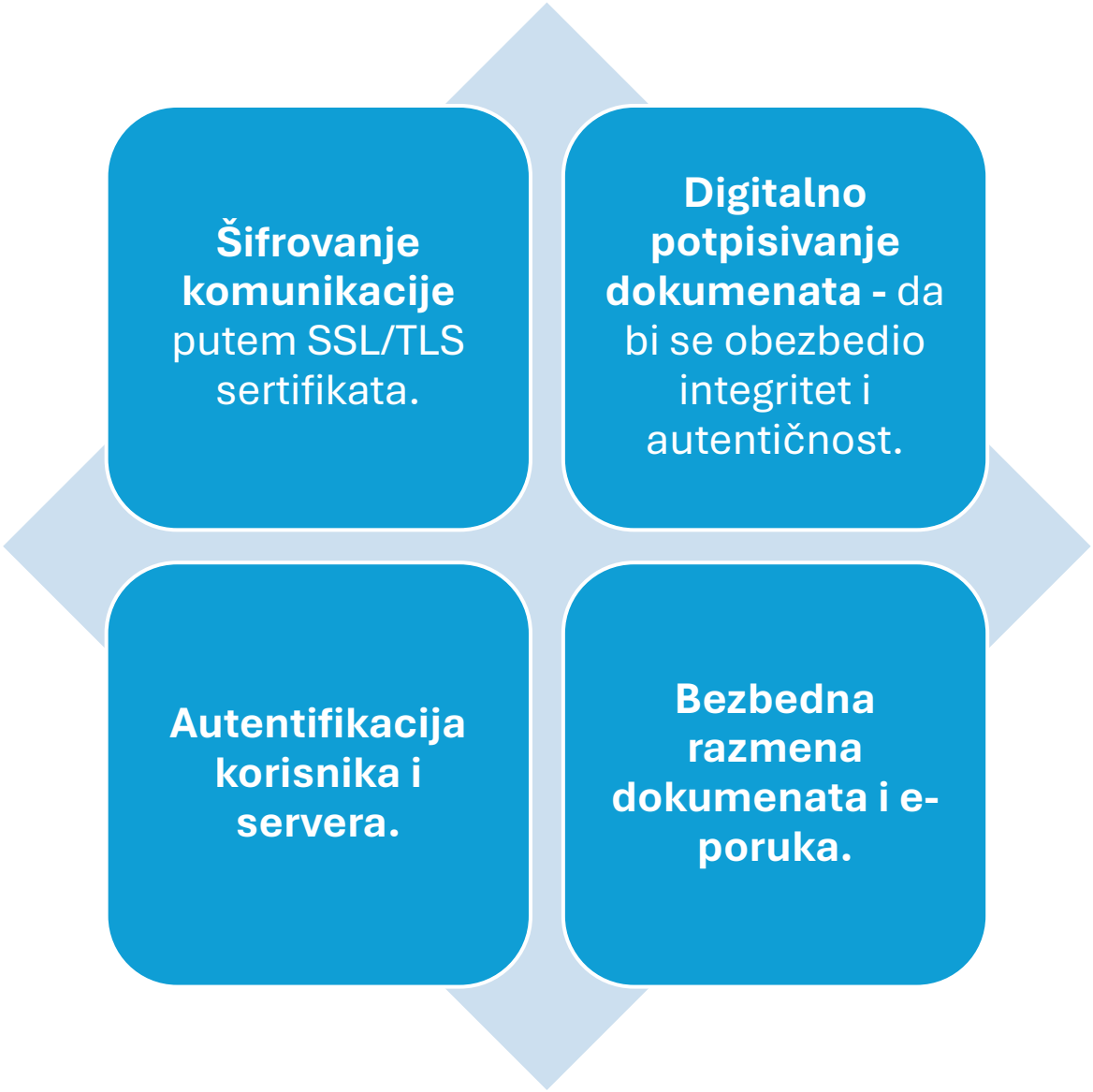
Glavne komponente PKI

1. **Par ključeva**
    1. **Javni ključ (Public Key) -**slobodno dostupan svima.
    2. **Privatni ključ (Private Key) -** tajan, čuva se kod vlasnika.
2. **Centralna autoritetna institucija – CA (Certificate Authority):**
   Organizacija koja izdaje digitalne sertifikate koji verifikuju identitet subjekta (npr. veb sajta, korisnika).
3. **Registracioni autoritet (RA – Registration Authority):**
   Potvrđuje identitet korisnika pre nego što CA izda sertifikat.
4. **Digitalni sertifikati (npr. X.509)**
   Dokumenti koji povezuju javni ključ sa identitetom vlasnika (npr. organizacije, sajta).
5. **CRL – Certificate Revocation List**
   Lista poništenih sertifikata koja se redovno ažurira.

Procesi u PKI

1. Generisanje ključeva
2. Izdavanje certifikata
3. Verifikacija identiteta
4. Revokacija certifikata

Upotreba PKI u e-poslovanju



Doprinos PKI

poverenje među učesnicima u e-trgovini,

pouzdanu verifikaciju identiteta,

siguran prenos podataka.